

P-2297

(19)日本国特許庁 (J P) (2) 公開特許公報 (A)

(11)特許出願公開番号  
特開2001-14871  
(P2001-14871A)  
(43)公開日 平成13年1月19日(2001.1.19)

(5)Int.Cl. <sup>7</sup>	識別記号	PI	チーフド(参考)
G11C 16/02		G11C 17/00	601P 5B017
G06F 12/14	310	G06F 12/14	310B 5B025
	320		310F
			320D

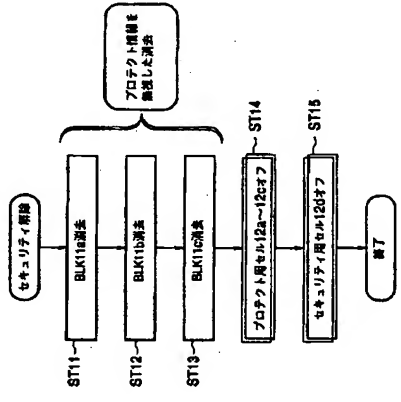
審査請求 未請求 請求項の数 9 OI (全 8 頁)

(21) 出願番号	特願平11-183228	(71) 出願人	000030378 株式会社東芝
(22) 出願日	平成11年6月29日(1999.6.29)	(72) 発明者	神奈川県川崎市幸区堀川町72番地 株 西 央 倫 神奈川県川崎市幸区小向東芝町1番地 株 式会社東芝マイクroeレトロニクスセン ター内
		(73) 発明者	西村 望 神奈川県川崎市幸区小向東芝町1番地 株 式会社東芝マイクroeレトロニクスセン ター内
		(74) 代理人	100058479 弁理士 鈴江 武彦 (外6名)

最終頁に続く

(54)【発明の名称】 不揮発性半導体記憶装置

(57)【要約】  
【課題】本発明は、セキュリティ機能およびプロテクト機能を備えるフラッシュメモリにおいて、セキュリティ機能の解除方法が知られた場合にも、保持データが推定・漏洩されるのを防止できるようにすることを最も主要な特徴とする。  
【解決手段】たとえば、誤書き込みなどによる保持データの破壊を防止するために、プロテクト情報/セキュリティ情報記憶回路内のプロテクト用セルによってプロテクト情報が設定されている状態において、セキュリティ機能の解除が指示されたとする。すると、プロテクト用セルによるプロテクト情報の推定を無視して、各ブロック内のすべての保持データを強制的に消去する。この後、セキュリティ情報の設定を解除することによって、第三者によってセキュリティ機能が解除されたとしても、保持データが外部に漏れるのを防ぐ構成となっている。



【特許請求の範囲】  
【請求項1】 保持データを記憶する、書き換え可能なメモリ手段と、  
このメモリ手段における、前記保持データの書き換えを禁止するための書き換え禁止情報を設定することが可能な書き換え禁止手段と、  
前記メモリ手段からの、前記保持データの読み出しを禁止するための読み出し禁止情報を設定することが可能な読み出し禁止手段と、  
この読み出し禁止手段での前記読み出し禁止情報の設定による読み出し禁止状態を解除する際、前記書き換え禁止手段での前記書き換え禁止情報の設定にかかわらず、前記メモリ手段における前記保持データを消去する消去手段とを具備したことを特徴とする不揮発性半導体記憶装置。

記憶読み出し禁止情報の設定を解除する解除手段とを具備したことを特徴とする不揮発性半導体記憶装置。

【請求項7】 前記メモリ手段は、記憶エリアが複数のブロックに分割され、各エリアごとに前記書き換え禁止手段による書き換え禁止情報の設定が可能であることを特徴とする請求項6に記載の不揮発性半導体記憶装置。  
【請求項8】 前記書き換え禁止手段および前記読み出し禁止手段は、前記メモリ手段内に設けられることを特徴とする請求項7に記載の不揮発性半導体記憶装置。  
【請求項9】 前記解除手段は、さらに、前記メモリ手段における前記保持データが消去された後に、前記書き換え禁止手段での前記書き換え禁止情報の設定を解除せしめることを特徴とする請求項6に記載の不揮発性半導体記憶装置。

【請求項10】 前記書き換え禁止手段は、さらに、前記メモリ手段における前記保持データが消去された後に、前記書き換え禁止手段での前記書き換え禁止情報の設定を解除せしめることを特徴とする請求項6に記載の不揮発性半導体記憶装置。  
【請求項11】 前記書き換え禁止手段は、さらに、前記メモリ手段における前記保持データが消去された後に、前記書き換え禁止手段での前記書き換え禁止情報の設定を解除せしめることを特徴とする請求項6に記載の不揮発性半導体記憶装置。

【発明の詳細な説明】

【0001】  
【発明の属する技術分野】この発明は、不揮発性半導体記憶装置に関するもので、特に、セキュリティ機能およびプロテクト機能を備えるフラッシュメモリ (Flash EEPROM (Electrically Erasable Programmable Read Only Memory)) に関するものである。

【0002】  
【従来の技術】周知のように、不揮発性半導体記憶装置としては、ユーザによるオンボード (On-board) の書き換えが可能なフラッシュメモリがあげられる。このフラッシュメモリには、保持データの推定・漏洩を防ぐために、保持データの書き換えを禁止する手段 (以下、プロテクト機能) および、保持データの読み出しを禁止する手段 (以下、セキュリティ機能) を有するものがある。

【0003】以下に、従来のフラッシュメモリにおける、プロテクト機能/セキュリティ機能の基本的概念について説明する。  
【0004】図4は、従来のフラッシュメモリにおけるプロテクト機能の基本的概念を示すものである。  
【0005】たとえば、フラッシュメモリ本体101に、保持データを書き換え禁止 (プロテクト、オフ) 状態または書き換え許可 (プロテクト、オン) 状態を設定するためのプロテクト情報は、フラッシュメモリ本体101とは別の、専用のフラッシュメモリ (Fuse Cell Array) となるプロテクト情報記憶回路102内に記憶されるようになっている。

【0006】そして、保持データの書き換え/消去時には、たとえば、ステートマシン103内の、アドレス103aによる、コマンドインターフェイス104からの信号と上記プロテクト情報記憶回路102内のプロテクト情報とのアンド出力にたがって、書き込み/消去制御回路103bが制御されるように構成されている。  
【0007】すなわち、上記プロテクト情報記憶回路102内のプロテクト情報として、たとえば「1」が記憶

【請求項5】 前記消去手段は、前記メモリ手段における前記保持データを消去した後に、前記読み出し禁止手段での前記読み出し禁止情報の設定、および、前記書き換え禁止手段での前記書き換え禁止情報の設定を、それぞれを解除せしめることを特徴とする請求項1に記載の不揮発性半導体記憶装置。  
【請求項6】 保持データを記憶する、書き換え可能なメモリ手段と、  
このメモリ手段における、前記保持データの書き換えを禁止するための書き換え禁止情報を設定することが可能な書き換え禁止手段と、  
前記メモリ手段からの、前記保持データの読み出しを禁止するための読み出し禁止情報を設定することが可能な読み出し禁止手段と、  
この読み出し禁止手段での前記読み出し禁止情報の設定による読み出し禁止状態を解除する際、前記書き換え禁止手段での前記書き換え禁止情報の設定にかかわらず、前記メモリ手段における前記保持データを消去する消去手段とを具備したことを特徴とする不揮発性半導体記憶装置。

【請求項7】 前記書き換え禁止手段は、さらに、前記メモリ手段における前記保持データが消去された後に、前記書き換え禁止手段での前記書き換え禁止情報の設定を解除せしめることを特徴とする請求項6に記載の不揮発性半導体記憶装置。  
【請求項8】 前記書き換え禁止手段は、さらに、前記メモリ手段における前記保持データが消去された後に、前記書き換え禁止手段での前記書き換え禁止情報の設定を解除せしめることを特徴とする請求項6に記載の不揮発性半導体記憶装置。

【請求項9】 前記書き換え禁止手段は、さらに、前記メモリ手段における前記保持データが消去された後に、前記書き換え禁止手段での前記書き換え禁止情報の設定を解除せしめることを特徴とする請求項6に記載の不揮発性半導体記憶装置。  
【請求項10】 前記書き換え禁止手段は、さらに、前記メモリ手段における前記保持データが消去された後に、前記書き換え禁止手段での前記書き換え禁止情報の設定を解除せしめることを特徴とする請求項6に記載の不揮発性半導体記憶装置。

【請求項11】 前記書き換え禁止手段は、さらに、前記メモリ手段における前記保持データが消去された後に、前記書き換え禁止手段での前記書き換え禁止情報の設定を解除せしめることを特徴とする請求項6に記載の不揮発性半導体記憶装置。

されて、プロテクト、オフが設定されているとすると、上記コマンドインターフェイス104からの信号の供給にもなっており、上記アンド回路103aからの書き換え信号(アンド出力)が「1(許可)」となる。これにより、ステートマシン103による、フラッシュメモリ本体101に対する保持データの書き込み/消去が許可される。

【0008】一方、上記プロテクト情報記憶回路102内に「0」が記憶されて、プロテクト、オンが設定されている場合には、上記コマンドインターフェイス104からの信号の供給にかかわらず、上記アンド回路103aからの書き換え信号が「0(不可)」となる。これにより、フラッシュメモリ本体101に対する保持データの書き込み/消去が禁止される。

【0009】プロテクト機能とは、こうしたプロテクト情報に応じて、フラッシュメモリ本体101に対する保持データの書き込み/消去の許可/禁止を制御することとで、正規ユーザ以外の第三者による保持データの捏造を防止するものである。

【0010】また、このようなプロテクト機能は、フラッシュメモリ本体の記憶エリア(アドレス領域)が複数ブロックに分隔されているフラッシュメモリにおいては、各ブロックごとにプロテクト情報を設定することが可能とされる場合が多い。

【0011】たとえば、記憶エリアが複数のブロックに分隔されているフラッシュメモリ本体のあるブロック(BLK0)内に保持しているデータは書き換え頻度の少ない(または、重要)プログラムであり、別のブロック(BLK1)内に保持しているデータは書き換え頻度の多いデータであるとする、書き込み込みなどによるデータの破壊がシステムの致命傷となるため、この場合、ブロック(BLK0)に対してはプロテクト、オンとし、ブロック(BLK1)に対してはプロテクト情報の設定が面倒(W/E時間の増加)などの理由から、プロテクト、オフとするといった使用例がある。

【0012】図5は、従来のフラッシュメモリにおけるセキュリティ機能の基本概念を示すものである。【0013】たとえば、フラッシュメモリ本体101に対する保持データの読み出し禁止(セキュリティ、オン)状態または読み出し許可(セキュリティ、オフ)状態を設定するためのセキュリティ情報は、フラッシュメモリ本体101とは別の、専用のフラッシュメモリ(Fuse Cell Array)からなるセキュリティ情報記憶回路105内に記憶されるようになっている。

【0014】そして、保持データの読み出し時には、たとえば、データ制御回路106内の、アンド回路106aによる、読み出し制御回路106bからの信号と上記セキュリティ情報記憶回路105内のセキュリティ情報とのアンド出力にしたがって、読み出し回路107とデータ出力端子Doutとの間の設けられたトライステート

リテリ情報記憶回路105を構成するセル102dの選択が行われた後に、該セル102dに対するオン/オフの設定が行われる。

【0024】しかしながら、このような構成のフラッシュメモリにおいては、セキュリティ情報は、セキュリティリテリ、オン)することによって、保持データの捏造・漏洩を防止できるもの、セキュリティ機能の解除方法が知られた場合には、第三者に保持データが容易に捏造・漏洩される可能性があるというデメリットがある。

【0025】図7は、従来のフラッシュメモリにおける、セキュリティ機能の解除動作にかかる処理の流れを示すものである。

【0026】たとえば、誤書き込みなどによる保持データの破壊を防止するために、全ブロックBLKについて、プロテクト情報が設定(プロテクト、オン)されている状態において、セキュリティ機能の解除(セキュリティ、オフ)が指示されたとする。

【0027】すると、セキュリティ情報の設定を解除するためにセキュリティ用セルをオフにするが、この場合、まず、各ブロックBLKのプロテクト情報の設定を順にチェックして、プロテクト、オフのプロテクトBLK内の保持データのみ、順次、消去する(ステップSTO1〜STO3)。

【0028】しかる後、セキュリティ情報の設定を解除して(ステップSTO4)、一連の動作を終了する。

【0029】すなわち、プロテクト情報が設定されている場合には、そのブロックBLK内の保持データの消去を行い、プロテクト情報が設定されている場合には、そのブロックBLK内の保持データの消去を行わずに、セキュリティ情報の設定が解除される。

【0030】この場合、保持データが失われるまま、該保持データの読み出しが可能となる状態となる。その結果、セキュリティ機能の解除が第三者により行われた場合には、保持データの内容が第三者に知られることになる。

【0031】なお、保持データを読み出した後には、再度、当該ブロックBLK内にデータを書き込む必要があるため、プロテクト用セルをオフにして、プロテクト機能を解除する。

【0032】そして、当該ブロックBLK内にデータを書き込んだ後、必要に応じて、プロテクト情報の設定(プロテクト、オン)が行われる。

【0033】このように、従来の、セキュリティ機能の解除の方法が知られてしまった場合には、第三者による保持データの改ざん(捏造)までもが容易に可能となり、プロテクト機能/セキュリティ機能は全く意味のないものとなるという問題があった。

【0034】

【発明が解決しようとする課題】上記のように、従来の保持データは、セキュリティ機能の解除方法が知られた場

合には、第三者に保持データが容易に捏造・漏洩される可能性があるという問題があった。

【0035】そこで、この発明は、セキュリティ機能の解除方法が知られた場合にも、保持データが捏造・漏洩されるのを防止でき、保持データの秘密性を飛躍的に向上させることが可能な不揮発性半導体記憶装置を提供することを目的としている。

【0036】

【課題を解決するための手段】上記の目的を達成するために、この発明の不揮発性半導体記憶装置においては、保持データを記憶する、書き換え可能なメモリ手段と、このメモリ手段における、前記保持データの書き換えを禁止するための書き換え禁止情報を設定することが可能な書き換え禁止手段と、前記メモリ手段からの、前記保持データの読み出しを禁止するための読み出し禁止情報を設定することが可能な読み出し禁止手段と、この読み出し禁止手段での前記読み出し禁止情報の設定による読み出し禁止状態を解除する際、前記書き換え禁止手段での前記書き換え禁止情報の設定にかかわらず、前記メモリ手段における前記保持データを消去する消去手段とから構成されている。

【0037】また、この発明の不揮発性半導体記憶装置においては、保持データを記憶する、書き換え可能なメモリ手段と、このメモリ手段における、前記保持データの書き換えを禁止するための書き換え禁止情報を設定することが可能な書き換え禁止手段と、前記メモリ手段からの、前記保持データの読み出しを禁止するための読み出し禁止情報を設定することが可能な読み出し禁止手段と、この読み出し禁止手段での前記読み出し禁止情報の設定による読み出し禁止状態を解除する際に、前記書き換え禁止手段での前記書き換え禁止情報の設定による書き換え禁止状態を判断する判断手段と、この判断手段により書き換え禁止状態が判断された場合、前記メモリ手段における前記保持データを消去する消去手段と、この消去手段により、前記メモリ手段における前記保持データが消去された後に、前記読み出し禁止手段での前記読み出し禁止情報の設定を解除する解除手段とから構成されている。

【0038】この発明の不揮発性半導体記憶装置によれば、書き換え禁止情報の設定にかかわらず、読み出し禁止情報の設定が解除された場合には、メモリ手段における保持データを消去できるようにする。これにより、たとえ第三者が読み出し禁止情報の設定を解除する方法を知ったとしても、保持データが第三者の目に触れるのを避けることが可能となるものである。

【0039】

【発明の実施の形態】以下、この発明の実施の形態について図面を参照して説明する。

【0040】(一実施形態)図1は、本発明の一実施形態にかかるとる不揮発性半導体記憶装置の概略構成を、フラ

ッシュメモリ (Flash EEPROM) を例に示すものである。

【0041】このフラッシュメモリは、たとえば、フラッシュメモリ本体 (書き換え可能なメモリ手段) 1、プロテクト情報/セキュリティ情報記憶回路12、コマンドインターフェース13、ステートマシン (消去手段) 14、データ制御回路15、読み出し回路16、トライステート・バッファ17、および、電源回路18を有して構成されている。

【0042】フラッシュメモリ本体11は保持データを記憶するためのもので、たとえば、記憶エリア (全アドレス領域) が3つのブロック (BLK) 11a, 11b, 11cに分割されている。

【0043】プロテクト情報/セキュリティ情報記憶回路12は、たとえば、上記フラッシュメモリ本体11とは別、専用のフラッシュメモリ (Fuse Cell Array) からなり、プロテクト機能 (書き換え禁止手段) として、上記各ブロック11a, 11b, 11cにおける保持データの書き換えを禁止するためのプロテクト情報 (書き換え禁止情報) をそれぞれ記憶するプロテクト用セル12a, 12b, 12cを、セキュリティ機能 (書き出し禁止手段) としての、上記全ブロック11a, 11b, 11cに対する保持データの読み出しを禁止するためのセキュリティ情報 (読み出し禁止情報) を記憶するセキュリティ用セル12dとを有して構成されている。

【0044】コマンドインターフェース13は、たとえば、アウトプット・インポート信号入力端子 (I/OE)、チップ・インポート信号入力端子 (ICE)、ライト・インポート信号入力端子 (IWE)、ブロック情報 (アドレス) 入力端子Add、および、データ入力端子 (Data) を介して、それぞれ外部より供給される情報にもついで、上記フラッシュメモリ本体11に対するデータの読み出し、書き込み、消去を判断し、上記ステートマシン14を制御するものである。

【0045】ステートマシン14は、上記コマンドインターフェース13の制御のもと、上記プロテクト情報/セキュリティ情報記憶回路12内に記憶されているプロテクト情報の設定に応じて、上記フラッシュメモリ本体11に対するデータの書き込み/消去を実行するものである。

【0046】また、ステートマシン14は、たとえば図5に示すように、セキュリティ機能の解除 (セキュリティ、オフ) が指示された場合には、上記プロテクト情報/セキュリティ情報記憶回路12内のプロテクト用セル12a~12cをチェックして、プロテクト情報の設定により書き換え禁止 (プロテクト、オン) 状態を判断し、書き換え禁止状態であれば、該プロテクト情報の設定を無視して、上記フラッシュメモリ本体11内の全ブロック11a~11cにおける保持データの消去を行

う (図3参照)。たとえばプロテクト用セルによつて書き換え禁止状態が設定されている場合であっても、その設定にかかわらず、当該ブロック内で保持されているデータの消去を可能にすることである。

【0056】全ブロック11a~11c内のすべての保持データを消去し終えた後においては、解除手段としての書き込み/消去回路 (図6参照) により、プロテクト用セル12a~12cをオフにして、プロテクト情報の設定を解除し、これによりプロテクト機能を解除する (ステップST14)。

【0057】正規のユーザは、新たに所持しているデータをフラッシュメモリ本体11内に書き込む必要があるため、使い勝手を考えた場合、保持データの消去にもおのづかしく、プロテクト用セル12a~12cをオフにしておくのが良い (書き込みを行う際には、プロテクト用セルをオフにする必要があるため)。

【0058】また、解除手段としての書き込み/消去回路 (図6参照) により、セキュリティ用セル12dをオフにして、セキュリティ情報の設定を解除し、これによりセキュリティ機能を解除して (ステップST15)、一連の動作を終了する。

【0059】このように、セキュリティ機能の解除が指示された場合には、プロテクト情報の設定 (プロテクト、オン) にかかわらず、フラッシュメモリ本体11内の保持データをすべて消去した後に、セキュリティ情報の設定を解除 (セキュリティ、オフ) するようにしている。

【0060】したがって、保持データの読み出しが可能となつた際には、既に保持データが存在しない、その結果、たとえ何らかの手段によつて、何者かにセキュリティ機能の解除方法が知られたとしても、第三者による保持データの解除または改ざんは不可能となる。【0061】上記したように、プロテクト情報の設定にかかわらず、セキュリティ情報の設定が解除された場合には、フラッシュメモリ本体における保持データを消去できるようにしている。

【0062】すなわち、セキュリティ機能の解除が指示された場合には、フラッシュメモリ本体内の保持データをすべて消去した後に、セキュリティ情報の設定を解除するようにしている。これにより、たとえ何らかの手段によつて、何者かにセキュリティ機能の解除方法が知られたとしても、保持データが第三者の目に触れるのを避けることが可能となるため、第三者による保持データの解除または改ざんは不可能となる。したがって、正規のユーザ以外に、保持データが破壊・漏洩されるのを防止でき、保持データの秘密性を飛躍的に向上させることが可能となるのである。

【0063】特に、保持データの消去にもつて、プロテクト用セルをオフしてプロテクト情報の設定を解除するようにした場合には、正規ユーザの使い勝手をも向

上できる。

【0064】なお、上記したこの発明の一実施形態においては、プロテクト情報/セキュリティ情報記憶回路を、たとえば、フラッシュメモリ本体とは別の、専用のフラッシュメモリ (Fuse Cell Array) により構成するようにした場合には、プロテクト情報/セキュリティ情報記憶回路はフラッシュメモリ本体内に設けることも可能である。

【0065】また、保持データの保護・漏洩を防止する方法としては、上記した方法以外に、たとえば、プロテクト情報が設定されている保持データが存在する場合に、セキュリティ機能を解除できないようにするなどの方法も考えられる。

【0066】その他、この発明の要旨を変えない範囲において、種々変形実施可能なことは勿論である。【0067】

【発明の効果】以上、詳述したようにこの発明によれば、セキュリティ機能の解除方法が知られた場合にも、保持データが破壊・漏洩されるのを防止でき、保持データの秘密性を飛躍的に向上させることが可能な不揮発性半導体記憶装置を提供できる。

【図面の簡単な説明】

【図1】この発明の一実施形態にかかる、フラッシュメモリの回路構成を示すブロック図。

【図2】同じく、フラッシュメモリにおける、セキュリティ機能の解除動作にかかる処理の流れを示すフローチャート。

【図3】同じく、フラッシュメモリにおける、保持データの消去動作にかかる処理の流れを示すフローチャート。

【図4】従来の技術とその問題点を説明するために、フラッシュメモリにおけるプロテクト機能の基本的概念を示すブロック図。

【図5】同じく、従来のフラッシュメモリにおけるセキュリティ機能の基本的概念を示すブロック図。

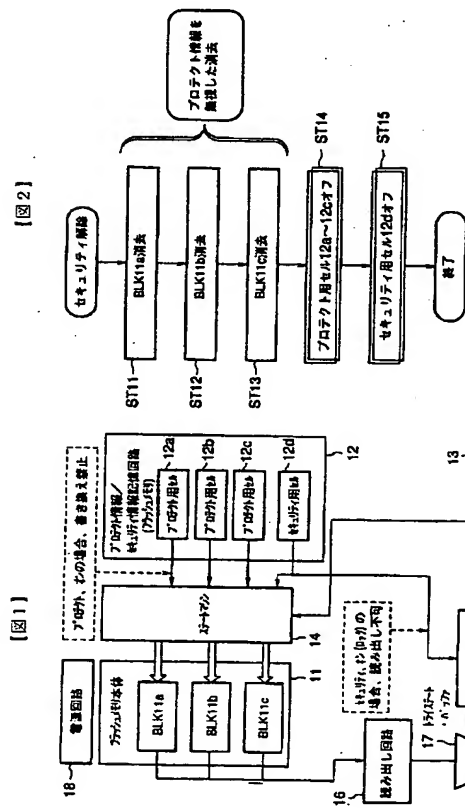
【図6】同じく、プロテクト情報およびセキュリティ情報の設定方法を説明するために、フラッシュメモリの要部の構成を概略的に示すブロック図。

【図7】同じく、従来のフラッシュメモリにおける、セキュリティ機能の解除動作にかかる処理の流れを示すフローチャート。

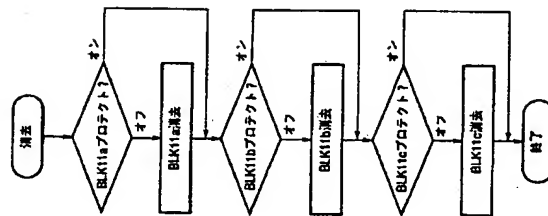
【符号の説明】

11...フラッシュメモリ本体  
11a, 11b, 11c...ブロック  
12...プロテクト情報/セキュリティ情報記憶回路  
12a, 12b, 12c...プロテクト用セル  
12d...セキュリティ用セル  
13...コマンドインターフェース  
14...ステートマシン  
15...データ制御回路

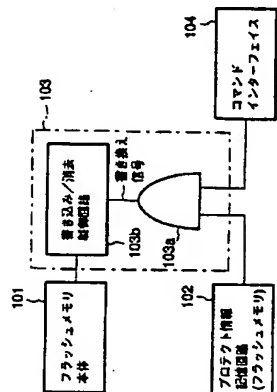
16...読み出し回路  
17...トライステート・バッファ  
18...電源回路  
ノOE...アウトプットネーブル信号入力端子  
ノCE...チップイネーブル信号入力端子  
ノWE...ライトイネーブル信号入力端子  
Add...ブロック情報入力端子  
Din...データ入力端子  
Dout...データ出力端子



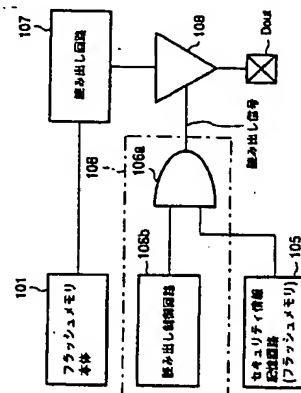
【図3】



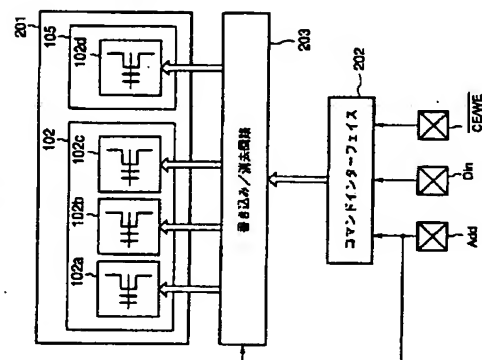
【図4】



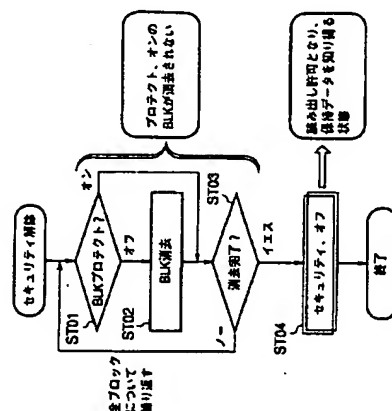
【図5】



【図6】



【図7】



フロントページの続き

Fターム(参考) 58017 A02 A03 A06 BA04 BA08  
BA10 BB03 BB05 CA12 CA16  
58025 A03 AB01 AC01 AD08 AD14  
AE10

**Nonvolatile semiconductor memory device with security function and protect function**

Patent Number: ☐ US6229731  
Publication date: 2001-05-08  
Inventor(s): KASAI NOZOMI (JP); KASAI TAKAMICHI (JP)  
Applicant(s): TOKYO SHIBAURA ELECTRIC CO (US)  
Requested Patent: ☐ JP2001014871  
Application Number: US20000606146 20000629  
Priority Number(s): JP19990183228 19990629  
IPC Classification: G11C16/04  
EC Classification: G11C16/22  
Equivalents:

---

**Abstract**

---

The invention provides a flash memory having a security function and a protect function. When the release of the security function has been instructed, all data stored in each block of a flash memory main body is forcibly erased, ignoring the setting of the protect function. After that, the security function is released, thereby enabling readout of data. This being so, even if a third person releases the security function, leakage of data to the outside can be prevented

---

Data supplied from the esp@cenet database - I2